

AN: PAT 1986-138240
TI: Input-output failure protection for multiprocessor system
transmitting data over duplicated channels with facility to
identify faulty unit
PN: DE3442418-A
PD: 22.05.1986
AB: The multiprocessor has duplicated redundancy built in to
provide safe operation. A number of processors (RS1-RS6) have
duplicated input/output units (E/A21, E/A22, etc.) that are led
to two buses (B1, B2). A digital data from one processor (RS2)
to another (RS1) is either transmitted in identical form or in
true and inverted form by the I/O stages (E/A21, E/A22). Upon
reception the data is subjected to a checking procedure. Any
fault in the I/O unit is signalled back to the transmitting
processor. Any further transmissions are switched to an
alternative processor that has correctly operating I/O units.;
To control railway network switching system.
PA: (SIEI) SIEMENS AG;
IN: GUNTHER R; LOHMANN H J;
FA: DE3442418-A 22.05.1986; DE3585361-G 19.03.1992;
EP182134-A 28.05.1986; EP182134-B 05.02.1992;
CO: AT; CH; DE; EP; LI; NL;
DR: AT; CH; DE; LI; NL;
IC: G06F-011/16;
MC: T01-G03; T01-H01; T01-J02;
DC: T01;
PR: DE3442418 20.11.1984;
FP: 22.05.1986
UP: 19.03.1992

THIS PAGE BLANK (USPTO)

⑫

EUROPÄISCHE PATENTANMELDUNG

⑰ Anmeldenummer: 85113416.3

⑤① Int. Cl.: **G 06 F 11/00**

⑱ Anmeldetag: 22.10.85

③① Priorität: 20.11.84 DE 3442418

⑦① Anmelder: Siemens Aktiengesellschaft, Berlin und München Wittelsbacherplatz 2, D-8000 München 2 (DE)

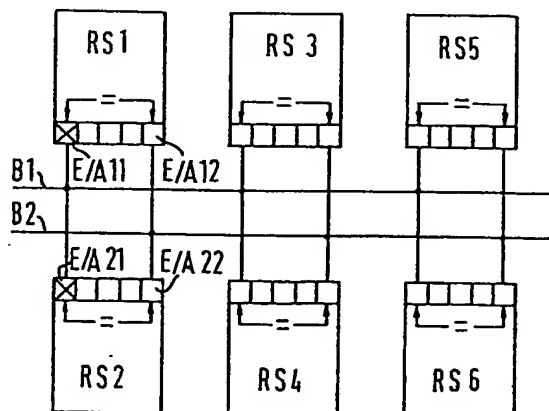
④③ Veröffentlichungstag der Anmeldung: 28.05.86
Patentblatt 86/22

⑦② Erfinder: Lohmann, Heinz-Jürgen, Dr.-Ing.,
Erfstasse 10, D-3300 Braunschweig (DE)
Erfinder: Günther, Rudolf, Dipl.-Ing., Ackerweg 25,
D-3300 Braunschweig (DE)

④④ Benannte Vertragsstaaten: AT CH DE LI NL

⑤④ Verfahren zum Betrieb eines signaltechnisch sicheren Mehrrechnersystems mit mehreren signaltechnisch nicht sicheren Ein/Ausgabebaugruppen.

⑤⑦ Das Mehrrechnersystem (RS1) prüft laufend die in den Ein/Ausgabebaugruppen (E/A11, E/A12) seiner Einzelrechner anstehenden, über gesonderte Kanäle übermittelten Daten auf Übereinstimmung. Beim Auftreten von Abweichungen führt das Mehrrechnersystem Redundanzprüfungen durch und ermittelt aus dem Ergebnis dieser Prüfungen die jeweils defekte Ein/Ausgabebaugruppe (z.B. E/A11). Für eine bestimmte Zeitspanne wird der Datenverkehr dann über eine noch intakte Ein/Ausgabebaugruppe (E/A12) abgewickelt. Die Datenübertragung während dieser Zeit erfolgt höherredundant als bei ordnungsgerechtem Zustand aller Ein/Ausgabebaugruppen.



Siemens Aktiengesellschaft
Berlin und München

Unser Zeichen
VPA 84 P 2938 E

5 Verfahren zum Betrieb eines signaltechnisch sicheren
Mehrrechnersystems mit mehreren signaltechnisch nicht
sicheren Ein/Ausgabebaugruppen

Die Erfindung bezieht sich auf ein Verfahren zum Be-
trieb eines signaltechnisch sicheren Mehrrechnersystems
10 mit mindestens zwei signaltechnisch nicht sicheren Ein/
Ausgabebaugruppen, über die die Rechner des Mehrrechner-
systems mindestens zweikanalig Datentelegramme von und/
oder zu anderen Rechnern und/oder sonstigen Daten auf-
15 nehmenden, abgebenden oder verarbeitenden Schaltmitteln
übertragen und über die sie von dort in Form von in-
haltlich übereinstimmenden Telegrammen für die Ein/Aus-
gabebaugruppen durch Prüfdaten gesicherte Nutzdaten emp-
fangen bzw. nach dort abgeben.

20 Für besonders sicherheitsrelevante Anwendungsfälle wie
z.B. das Eisenbahnsicherungswesen sind signaltechnisch
sichere Mehrrechnersysteme entwickelt worden, in denen
die zu verarbeitenden Daten in mehreren Kanälen jeweils
25 unabhängig voneinander nach bestimmten Gesetzmäßigkei-
ten behandelt werden; durch Vergleichsprozeduren werden
etwaige Datenabweichungen in den einzelnen Kanälen er-
kannt und in entsprechende Steuerkommandos umgesetzt,
die im Sinne eines Gefährdungsausschlusses auf den zu
30 steuernden Prozeß wirken. Signaltechnisch sichere Mehr-
rechnersysteme müssen aber nicht nur in der Lage sein,
die ihnen zugeführten Daten in der vorgegebenen Weise
zu behandeln, sondern sie müssen auch in der Lage sein
festzustellen, ob die in ihren signaltechnisch nicht

sicheren Ein/Ausgabebaugruppen anstehenden Daten beispielsweise infolge einer Übertragungsstörung oder eines Bauteiledefektes verfälscht sind oder nicht, um dann die Auswertung dieser verfälschten Daten zu unterbinden.

5

Ein bekanntes Verfahren zur Sicherung der Datenübermittlung sieht vor, den eigentlichen Nutzdaten sendeseitig nach bestimmten Gesetzmäßigkeiten gebildete Prüfdaten beizugeben, aus den übermittelten Nutzdaten empfangsseitig nach den gleichen Gesetzmäßigkeiten die zugehörigen Prüfdaten nachzubilden und diese mit den übermittelten Prüfdaten zu vergleichen. Diese Art der Datensicherung ist im allgemeinen um so wirkungsvoller, je aufwendiger die Prüfdaten werden.

15

Bei der heutigen Technik sind die Ein/Ausgabebaugruppen elektronischer Datenverarbeitungseinrichtungen üblicherweise mit hochintegrierten Schaltkreisen (FIFOS) besetzt, deren mögliche Ausfallreaktionen nicht umfassend bekannt sind und aus Aufwandsgründen auch nicht durch Analyse ermittelt werden können. Dies hat zur Folge, daß der Nachweis dafür, daß es keine Ausfallwirkung gibt, die trotz Redundanzprüfung unerkannt bleibt, in letzter Konsequenz nicht vollständig geführt werden kann, so daß auch bei sehr umfangreichen Prüfdaten nicht erkennbare Nutzdatenverfälschungen nicht ausgeschlossen werden können. Deshalb erfüllt dieses Lösungskonzept die Forderungen hinsichtlich signaltechnischer Sicherheit als Voraussetzung für die Zulassung einer Telegrammübertragung für besonders sicherheitsrelevante Anwendungen nur unzureichend.

30

Nicht vorhersagbare Ausfallreaktionen einer Baugruppe, z.B. einer mit hochintegrierten Schaltkreisen bestückten

- Ein/Ausgabebaugruppe, lassen sich grundsätzlich durch Vervielfachung dieser Baugruppen und Vergleich ihrer Reaktionen miteinander erkennen. Für den vorliegenden Anwendungsfall bedeutet dies, daß die ein-bzw. auszu-
- 5 gebenden Informationen jeweils parallel in mindestens zwei gesonderte Ein/Ausgabebaugruppen einzuschreiben sind und daß das Mehrrechnersystem dann die gegenseitige Übereinstimmung der abgespeicherten Daten überprüft. Wird beim Vergleich der in diesen Baugruppen gespeicherten
- 10 ten Daten eine Ungleichheit erkannt, so sperrt das Rechnersystem die Verwertung der gespeicherten Informationen. Damit ist die Ungefährlichkeit des ersten Ausfalls einer Ein/Ausgabebaugruppe absolut gegeben.
- 15 Ein Defekt an einer Ein/Ausgabebaugruppe soll zwar als solcher sofort erkannt und in seiner Auswirkung unwirksam gemacht werden; ein derartiger Defekt soll jedoch nach Möglichkeit nicht den weiteren Datenverkehr des Rechnersystems mit den Systemelementen blockieren, die
- 20 die durch den Defekt betroffene Ein/Ausgabebaugruppe mit Daten versorgen bzw. von dort Daten beziehen und er soll insbesondere nicht zum Ausfall des gesamten Rechnersystems führen. Um den Datenverkehr auch beim Ausfallen einzelner Ein/Ausgabebaugruppen fortführen zu können,
- 25 ist es bekannt, jeder Ein/Ausgabebaugruppe mindestens eine entsprechende Reservebaugruppe beizuordnen, die spätestens im Störfall zu aktivieren ist und dann die Datenübertragung übernimmt.
- 30 Nachteilig an dieser Ausführung ist der hohe Aufwand für die Ein/Ausgabebaugruppen. Dies ist besonders schwerwiegend, wenn es sich bei den Ein/Ausgabebaugruppen um die Schnittstellen zu vielen anderen Rechnern oder sonstigen Anlagenelementen mit gleichen Anforderungen han-

delt. Dann muß nämlich dieser zusätzliche Aufwand an allen Rechnern getrieben werden und das geht erheblich ins Geld.

- 5 Eine Möglichkeit, die beiden vorgenannten Sicherungsmethoden miteinander zu verknüpfen, besteht darin, die zu übermittelnden Daten mit Prüfdaten zu versehen und mehrkanalig auszuwerten. Dieses Verfahren wird bei der in der DE-OS 26 09 107 offenbarten Schaltung angewandt.
- 10 Nach Prüfung der Redundanz in mehreren voneinander unabhängigen Baugruppen werden die von diesen Baugruppen gebildeten Ergebnisse miteinander verglichen. Wenn man davon ausgeht, daß - wie bereits dargelegt - durch Redundanzprüfungen Datenverfälschungen in einem Register
- 15 nicht mit absoluter Sicherheit erkannt werden können, dann können derartige Verfälschungen auch nicht durch eine verdoppelte Redundanzprüfung sicher aufgezeigt werden. Das bedeutet, daß die aus der DE-OS 26 09 107 bekannte Schaltung den hohen Sicherheitsanforderungen signaltechnisch sicherer Mehrrechnersysteme nicht gerecht
- 20 wird.

- Aufgabe der vorliegenden Erfindung ist es, Verfahren zum Betrieb eines signaltechnisch sicheren Mehrrechnersystems
- 25 gemäß dem Oberbegriff des Patentanspruches 1 bzw. 2 anzugeben, die etwaige Datenverfälschungen in bestimmten, durch inhaltlich gleiche Datentelegramme beschickten Ein/Ausgabebaugruppen sicher erkennen, um sie in ihrer Auswirkung unwirksam zu machen und die es darüber hinaus
- 30 gestatten, den Datenverkehr auch nach dem Auftreten einer Datenverfälschung mindestens bedingt aufrechtzuerhalten, ohne daß es hierzu der Bereitstellung zusätzlicher Reservebaugruppen bedarf. Die erfindungsgemäßen Verfahren sollen dabei in sich so transparent sein, daß

der Nachweis für den sicheren Zugriff von Datenverfälschungen als Voraussetzung für die Zulassung der erfindungsgemäßen Verfahren bei sicherheitsrelevanten Anwendungen möglich ist. Ferner ist es Aufgabe der Erfindung, solche Einrichtungen zu benennen, die besonders geeignet sind für die Durchführung der erfindungsgemäßen Verfahren.

Die Erfindung löst diese Aufgabe durch die kennzeichnenden Merkmale des Patentanspruches 1 bzw. die des Patentanspruches 2. Vorteilhafte Aus- und Weiterbildungen der Erfindung sind in den Unteransprüchen angegeben.

Beide Verfahren sind so beschaffen, daß sie auf in den mit übereinstimmenden Datentelegrammen zu belegenden Ein/Ausgabebaugruppen eines Mehrrechnersystems auftretende Datenverfälschungen sicher reagieren, die Auswertung der fehlerbehafteten Daten verhindern und die an der Datenverfälschung tatsächlich oder möglicherweise beteiligten Elemente von der weiteren Datenübermittlung ausschließen. Dabei führen die beiden Verfahren zu unterschiedlichen Reaktionen bezogen auf die Anzahl der von der jeweiligen Störung betroffenen Systemelemente. Nach beiden Verfahren wird die Datenübertragung im Anschluß an das Auffinden fehlerbehafteter Daten unter zusätzlicher Datensicherung und Belegung eines durch die Datenverfälschung nicht betroffenen Übertragungskanals für eine bestimmte Zeitspanne zugelassen, die zum Beheben des eingetretenen Defektes genutzt werden kann.

Die Erfindung ist nachstehend anhand von in der Zeichnung schematisch dargestellten Ausführungsbeispielen

näher erläutert.

Die Zeichnung zeigt in den Figuren 1 und 2 einen besonders vorteilhaften Aufbau von aus mehreren signaltech-
5 nisch sicheren Mehrrechnersystemen bestehenden Rechneranordnungen, die in unterschiedlicher Weise auf fehlerhaft abgelegte Daten reagieren, und in Figur 3 ein Funktionsschaubild zur Erläuterung der erfindungsgemäßen Verfahren bei einem signaltechnisch sicheren Zweirechner-
10 nersystem.

Die in Figur 1 dargestellte Rechneranordnung besteht aus beispielsweise sechs signaltechnisch sicheren Mehrrechnersystemen RS1 bis RS6, die über zugeordnete Ein/
15 Ausgabebaugruppen an die beiden Busse B1 und B2 eines Bussystems angeschlossen sind, über das die Mehrrechnersysteme zweikanalig miteinander kommunizieren. Es ist angenommen, daß das Rechnersystem RS2 Daten in Form eines Telegrammes an das Rechnersystem RS1 zu Übermitteln
20 hat. Hierzu aktiviert das Rechnersystem RS2 seine beiden Ein/Ausgabebaugruppen E/A21 und E/A22 zur beispielsweise adressenorientierten Übertragung inhaltlich gleicher Datentelegramme über die beiden Busse B1 und B2 an die Ein/Ausgabebaugruppen E/A11 und E/A12 des Rechnersystems
25 RS1; die über die beiden Busse übertragenen Datentelegramme können dabei unterschiedlich, z.B. invers dargestellt sein. Das die Daten aufnehmende Rechnersystem RS1 prüft die in seinen Ein/Ausgabebaugruppen abgelegten Daten vor ihrer Anerkennung auf Einhaltung des festgeleg-
30 ten Datenformates und auf inhaltliche Übereinstimmung. Dabei möge das Rechnersystem RS1 in seinen Ein/Ausgabebaugruppen E/A11 und E/A12 voneinander abweichende Daten feststellen. Das Rechnersystem verwirft daraufhin
35 das übermittelte Datentelegramm und fordert über beide

Busse B1, B2 vom Datensender, dem sicheren Mehrrechnersystem RS2, eine erneute Telegrammübertragung an. Gelingen die dabei übermittelten Daten den Prüfbedingungen des Rechnersystems RS1, so werden sie anerkannt, wobei
5 die Anerkennung der Daten dem Datensender quittiert werden kann. Endet auch der zweite Versuch einer Datenübermittlung negativ, d.h. stellt der Datenempfänger inhaltlich oder vom Format her abweichende Daten in seinen Ein/Ausgabebaugruppen fest, so stellt er auf noch zu erläutern-
10 de Weise fest, welcher der in seinen Ein/Ausgabebaugruppen abgelegten Datensätze fehlerhaft ist und welcher nicht. Im vorliegenden Beispiel möge das Rechnersystem RS1 die in seiner Ein/Ausgabebaugruppe E/A11 anstehenden Daten als fehlerhaft erkannt haben. Es sperrt
15 daraufhin rechnerintern die weitere Aufnahme von Daten über die betreffende Ein/Ausgabebaugruppe und unterrichtet mindestens das Mehrrechnersystem RS2, von dem das fehlerbehaftete Datentelegramm stammte, hiervon. Dies führt dort zum Setzen eines entsprechenden Sperrvermer-
20 kes, der die weitere Übertragung von Daten über die Ein/Ausgabebaugruppe E/A21 zur Ein/Ausgabebaugruppe E/A11 des Mehrrechnersystems RS1 verhindert. Damit wird dem Umstand Rechnung getragen, daß empfangsseitig zwar die aufgetretene Datenverfälschung erkennbar ist, nicht jedoch,
25 wo der Ort dieser Datenverfälschung liegt.

Wenn die von der festgestellten Störung direkt betroffenen beiden Rechnersysteme auch mit anderen, an das gleiche Bussystem angeschlossenen Rechnersystemen kommunizieren sollen, ist es vorteilhaft, auch diese Rechner
30 davon zu unterrichten, daß bestimmte Ein/Ausgabebaugruppen des die Störung feststellenden Rechnersystems und ggf. des Rechnersystems, von dem das verfälschte Datentelegramm stammte, für die weitere Datenübertragung

nicht mehr zur Verfügung stehen. Hierdurch soll verhindert werden, daß ein Defekt in einer einzigen Ein/Ausgabebaugruppe nach und nach zum Sperren weiterer Ein/Ausgabebaugruppen anderer Rechnersysteme führt.

5

Die durch die Störung direkt betroffenen Mehrrechnersysteme RS1 und RS2 korrespondieren untereinander und ggf. mit den durch die Störung nicht direkt betroffenen Mehrrechnersystemen RS3 bis RS6 fortan auf eine
10 Weise, wie sie im einzelnen anhand der Figur 3 erläutert wird.

Bei dem Ausführungsbeispiel der Figur 2 ist angenommen, daß auch das jeweils sendende Mehrrechnersystem die in
15 seinen Ein/Ausgabebaugruppen zur Übertragung anstehenden Daten vor der Übertragung auf Übereinstimmung prüft. Wieder soll dabei das sichere Mehrrechnersystem RS2 Datentelegramme über das Bussystem B1, B2 an das Mehrrechnersystem RS1 übermitteln. Beim Rücklesen der in den
20 Ein/Ausgabebaugruppen E/A21 und E/A22 anstehenden Daten möge das Mehrrechnersystem RS2 Abweichungen in den Daten feststellen. Die Ausgabe dieser Daten wird daraufhin verhindert und das Rechnersystem versucht - ggf. nach erneuter Generierung der entsprechenden Daten - auf noch
25 zu erläuternde Weise festzustellen, welcher der in seinen Ein/Ausgabebaugruppen anliegenden Datensätze fehlerhaft ist. Es möge dabei zu der Erkenntnis gelangen, daß die in seiner Ein/Ausgabebaugruppe E/A21 anliegenden Daten fehlerhaft sind. Das sichere Mehrrechnersystem veran-
30 laßt daraufhin durch Setzen einer entsprechenden Sperrmarkierung, daß über diese Ein/Ausgabebaugruppe keine weiteren Daten abgegeben werden; ggf. wird auch die Aufnahme von Daten über diese Ein/Ausgabebaugruppe gesperrt. Das Mehrrechnersystem RS2 unterrichtet die übrigen Mehr-

rechnersysteme von dieser Maßnahme und kommuniziert mit diesen Rechnersystemen fortan auf die nachstehend näher erläuterte Weise.

- 5 Die Zeichnung zeigt in Figur 3 ein Funktionsschaubild für die Erläuterung der erfindungsgemäßen Verfahren zum Betrieb eines Mehrrechnersystems, das durch zwei Einzelrechner R1 und R2 gebildet wird. In der Zeichnung sind nur diejenigen Elemente dargestellt, die für die
- 10 Erläuterung der erfindungsgemäßen Verfahren erforderlich sind. Die Ein- bzw. Ausgabe der hier interessierenden Daten erfolgt über zwei signaltechnisch nicht sichere Ein/Ausgabebaugruppen E/A1 und E/A2, die auf gesonderte Busse B1 und B2 geführt sind. Über diese Ein/Aus-
- 15 gabebaugruppen können sowohl Datentelegramme vom Rechnersystem aufgenommen als auch Daten an andere Rechner oder an eine Peripherie abgegeben werden. Die Daten setzen sich aus Nutz- und Prüfdaten zusammen.
- 20 Die bei der Eingabe von Daten in das Zweirechnersystem über die Busse B1, B2 zweikanalig angelieferten und in den Registern der Ein/Ausgabebaugruppen E/A1 und E/A2 anstehenden Daten werden im Zweirechnersystem jeweils vor ihrer Anerkennung miteinander verglichen, wobei sich
- 25 dieser Vergleich zunächst nur auf die Nutzdaten beschränken kann; es ist aber auch möglich, die jeweils übermittelten Daten grundsätzlich auch einer Redundanzprüfung zu unterziehen, d.h. die Zuordnung von Nutz- und Prüfdaten zu prüfen. Dieser Vergleich bzw. die zusätzliche
- 30 Redundanzprüfung findet dezentral in den beiden Einzelrechnern R1, R2 des sicheren Mehrrechnersystem statt. Jeder Einzelrechner vergleicht bzw. prüft die ihm von beiden Ein/Ausgabebaugruppen E/A1 und E/A2 angebotenen Datensätze. Stellen die Rechner unabhängig voneinander

- aber übereinstimmend abweichende Daten in den beiden Ein/Ausgabebaugruppen fest, so verwerfen sie die dort abgelegten Daten und fordern vom jeweiligen Datensender die erneute Übertragung der von ihnen als fehlerhaft erkannten Daten an. Genügen diese Daten den gegebenen Bewertungsbedingungen, so werden sie von den beiden Einzelrechnern akzeptiert und der weiteren Verarbeitung RV1, RV2 zugeführt.
- 10 Genügen die angeforderten Daten auch jetzt den gegebenen Bewertungsbedingungen nicht, so werden auch sie verworfen. Die beiden Einzelrechner R1, R2 versuchen nun festzustellen, welche der beiden Ein/Ausgabebaugruppen fehlerhafte Daten enthält und welche nicht. Hierzu unterziehen beide Rechner die ihnen von beiden Ein/Ausgabebaugruppen zugeführten Daten einer Redundanzprüfung. Dabei sollen beide Rechner übereinstimmend feststellen, daß der in einer Ein/Ausgabebaugruppe anstehende Datensatz den Redundanzbedingungen genügt, der andere jedoch
- 20 nicht. Im angenommenen Fall sollen beide Rechner die in der Ein/Ausgabebaugruppe E/A2 anliegenden Daten als fehlerhaft erkannt haben, während die in der Ein/Ausgabebaugruppe E/A1 anstehenden Daten den vorgegebenen Redundanzbedingungen genügen sollen.
- 25 Nach dem Vergleich ihrer Prüfergebnisse veranlassen beide Rechner das Setzen von Sperrmarkierungen und diese Sperrmarkierungen verhindern, daß die in der Ein/Ausgabebaugruppe E/A2 abgelegten Daten mindestens beim Datenverkehr mit demjenigen Element des Übertragungssystems,
- 30 von dem die Daten fehlerhaft empfangen bzw. abgelegt wurden, fortan ausgewertet bzw. fortgeschaltet werden. Dies geschieht z.B. dadurch, daß rechnerintern der Aufruf der als gestört erkannten Ein/Ausgabebaugruppe

zugeordneten Adresse verhindert wird. .

- Das die Störung erkennende Rechnersystem R1, R2 unterrichtet nun über das Bussystem die Datenquelle, von der die die Störung verursachenden Daten stammen, über die
- 5 eingetretene Störung und den durch die Störung betroffenen Übertragungskanal B1. Die jeweils angesprochene Datenquelle sperrt daraufhin ihrerseits die Auswertung bzw. Fortschaltung von Datentelegrammen über den gestörten Übertragungskanal B1. Die beiden durch die Störung
- 10 direkt betroffenen Rechnersysteme kommunizieren dann nur noch über mindestens einen durch die Störung nicht betroffenen Übertragungskanal, im angenommenen Beispiel über den Bus B2.
- Für den Fall, daß mindestens einer der beiden von der
- 15 Störung direkt betroffenen Mehrrechnersysteme über das Bussystem noch mit weiteren Rechnersystemen kommunizieren soll, ist es vorteilhaft, auch diese Rechner davon zu unterrichten, daß bestimmte Ein/Ausgabebaugruppen für die Datenübertragung nicht mehr zur Verfügung stehen.
- 20 [Gleichzeitig mit dem Setzen der Sperrmarkierung fordert das die Störung erkennende Rechnersystem das Rechnersystem, von dem die fehlerbehafteten Daten stammen, bzw. auch alle Rechnersysteme, mit denen es zu kommunizieren hat, dazu auf, zukünftig für die Übertragung von Daten
- 25 an das Rechnersystem R1, R2 höherredundante Daten zu erstellen und ausschließlich an die Ein/Ausgabebaugruppe E/A1 zu übertragen; entsprechend unterrichtet das sichere Mehrrechnersystem R1, R2 das bzw. die übrigen Mehrrechnersysteme davon, daß es selbst ebenfalls höherredundante Daten erstellen und diese über die Ein/Ausgabebaugruppe E/A1 an die Mehrrechnersysteme übermitteln
- 30 wird.

Die vorstehend erläuterten Maßnahmen können sinngemäß auch für einen Datensender gelten, von dem die als fehlerhaft erkannten Daten stammen.

- 5 Einzelne oder alle Mehrrechnersysteme überprüfen nun
fortlaufend bei Datenverkehr mit dem bzw. den durch die
Störung direkt betroffenen Mehrrechnersystemen das Ein-
halten der verschärften Redundanzbedingungen und sie
erstellen auch selbst für den Datenverkehr mit diesen
10 Mehrrechnersystemen die höherredundanten Daten. Entspre-
chendes gilt für die Mehrrechnersysteme mit den ausge-
fallenen Ein/Ausgabeeinrichtungen.

- Eine besonders bevorzugte Ausführungsform der Erfindung
15 sieht vor, daß die nach dem Ausfallen einer Ein/Ausgabe-
baugruppe zu übertragenden höherredundanten Datentele-
gramme das gleich Format wie die zuvor übertragenen
Datentelegramme aufweisen, daß sie aber von der jewei-
ligen Datenquelle her mehrfach übertragen werden, wobei
20 sich dann nicht ihr Inhalt aber ihre Darstellung ändert.
Vorzugsweise ist dabei an eine inverse Darstellung der
Daten in aufeinanderfolgenden Datentelegrammen gedacht.
Das jeweils als Empfänger fungierende sichere Mehrrech-
nersystem prüft vor der Anerkennung der Daten, ob in den
25 ihm nacheinander übermittelten Datentelegrammen sowohl
die Nutz- als auch die Prüfinformationen jeweils von
ihrem Inhalt her übereinstimmen und ob die übermittel-
ten Prüfinformationen mit den vom Rechnersystem nachge-
bildeten Prüfinformationen übereinstimmen. Nur solange
30 diese Voraussetzungen gegeben sind, ist die Auswertung
der von einem Rechnersystem mit einer defekten Ein/Aus-
gabebaugruppe stammenden Daten zulässig. Führt eine
Redundanzprüfung zu dem Ergebnis, daß entweder die nach-

- einander übermittelten Nutz- und Prüfinformationen nicht übereinstimmen oder daß die Zuordnung von Nutz- und Prüfinformationen nicht mehr gegeben ist, so wird der weitere Datenverkehr zum bzw. vom Mehrrechnersystem über die als gestört angesehenen Ein/Ausgabebaugruppen abgebrochen. Das Mehrrechnersystem mit den ausgefallenen Ein/Ausgabebaugruppen schaltet sich aber nur insoweit aus dem Rechnerverbund aus als die Datenübermittlung über die gestörten Ein/Ausgabebaugruppen betroffen ist; im übrigen arbeitet es nach wie vor weiter und setzt über andere Ein/Ausgabebaugruppen zugeführte Meldungen bestimmungsgemäß in entsprechende Kommandos um und überträgt diese Kommandos an die Prozeßperipherie.
- 15 Die Fortführung des Datenverkehrs über nur eine von zwei üblicherweise mit inhaltlich gleichen Datentelegrammen versorgte Ein/Ausgabebaugruppen ist nach der Lehre der vorliegenden Erfindung aber nicht für unbegrenzte Zeit zulässig, sondern diese Zeit ist auf eine maximal zulässige Zeitspanne begrenzt. Ist bis zu diesem Zeitpunkt die Störung durch Auswechseln oder Instantsetzen der gestörten Ein/Ausgabebaugruppe bzw. des Übertragungskanals nicht behoben, so verbietet sich die weitere Datenübertragung über das Bussystem. Die maximal zulässige Zeit für das Umschalten einer einzigen Ein/Ausgabebaugruppe auf beide Einzelrechner des Mehrrechnersystems ist abhängig von der für die betreffende Baugruppe aufgrund ihres Aufbaus zu erwartenden mittleren Zeit zwischen zwei unabhängig voneinander auftretenden Fehlern (MTBF = meantime between failures) und einer Kenngröße, die abhängig ist von der für die Datendarstellung erreichten Redundanz. Die erreichbare maximale Zeit, in der die Telegrammübertragung z.B. einkanalig betrieben werden darf, liegt bei einer typischen Rechneranordnung

mit einer Vielzahl von signaltechnisch sicheren Mehrrechner-
systemen in der Größenordnung von weit über
10 Stunden. In dieser Zeit, die rechnerisch bestimmt
werden kann, läßt sich der eingetretene Defekt durch
5 Instandsetzung oder durch Ersatz von Baugruppen mühe-
los beheben.

Für die Begrenzung der Zeitspanne, für die nach dem
Ausfallen einer Ein/Ausgabebaugruppe der Datenverkehr
10 über eine noch intakte Ein/Ausgabebaugruppe weiterge-
führt werden darf, ist dem sicheren Mehrrechnersystem
ein signaltechnisch sicheres Zeitglied zugeordnet. Die-
ses signaltechnisch sichere Zeitglied, das in der Zeich-
nung durch die Zeitglieder T1 und T2 verdeutlicht ist,
15 wird eingestellt, sobald die Rechner des Mehrrechner-
systems die Auswertung der in einer Ein/Ausgabebaugrup-
pe abgespeicherten Daten bleibend verhindern. Wird die
dem Zeitglied eingeprägte Schaltzeit überschritten, so
sperren die Rechner auch die Auswertung der noch in-
20 takten Ein/Ausgabebaugruppe. Diese Sperrung tritt auch
ein, wenn mindestens einer der Einzelrechner in den ihm
mitgeteilten höherredundanten Daten irgendwelche Feh-
ler entdeckt und wenn diese Fehler nicht durch nochma-
lige Datenübertragung zu beseitigen sind.

25 Für die Fortführung des Datenverkehrs nach dem Auftre-
ten einer Störung in einer Ein/Ausgabebaugruppe ist
ausschlaggebend, daß das betroffene Mehrrechnersystem
die defekte Ein/Ausgabebaugruppe beziehungsweise den
30 gestörten Datenkanal auch tatsächlich erkennt und nicht
etwa Daten aus der defekten Ein/Ausgabebaugruppe be-
ziehungsweise aus dem gestörten Datenkanal übernimmt.
Wie bereits erläutert wird die defekte und die intakte
Ein/Ausgabebaugruppe über Redundanzprüfungen ermittelt.

Dabei kann der Fall eintreten, daß nicht nur eine, sondern beide Redundanzprüfungen zu dem Ergebnis kommen, daß die jeweils übermittelten Prüfdaten mit den vom Mehrrechnersystem nachgebildeten Prüfdaten übereinstimmen. Dies ist möglich, wenn neben der Verfälschung von Nutzdaten im gleichen Kanal auch die übermittelten Prüfdaten gerade so verfälscht werden, daß sich daraus die für die verfälschten Nutzdaten richtigen Prüfdaten ergeben. Dieser Fall ist zwar sehr unwahrscheinlich, er ist jedoch nicht gänzlich auszuschließen. Tritt dieser Fall ein, so wird dies beim Vergleich der Redundanzprüfergebnisse festgestellt. Da die beiden Einzelrechner aus den Redundanzprüfungen in diesem Fall nicht den gestörten Übertragungskanal eindeutig bestimmen können, unterbinden sie in diesem Fall die weitere Datenübertragung über beide Ein/Ausgabebaugruppen.

Die vorstehend für Rechneranordnungen nach Figur 1 beschriebenen Abläufe gelten entsprechend auch für Rechneranordnungen gemäß Figur 2, bei denen die Rechner eines Mehrrechnersystems die in ihren Ein/Ausgabebaugruppen zur Übertragung anstehenden Datentelegramme vor ihrer Freigabe zurücklesen und die Freigabe vom Bilden übereinstimmender Prüfergebnisse in den Rechnern des Mehrrechnersystems abhängig machen.

Die erfindungsgemäßen Verfahren zum Betrieb eines signaltechnisch sicheren Mehrrechnersystems sind nicht auf die Ausbildung des sicheren Mehrrechnersystems als Zwei-von-Zwei/Rechnersystem beschränkt. Sie lassen sich vielmehr mit Vorteil bei jedem beliebigen signaltechnisch sicheren Mehrrechnersystem anwenden, das über mindestens zwei inhaltlich gleichen Datentelegrammen beschickte Ein/Ausgabebaugruppen mit anderen Rechnern oder mit

- der Peripherie kommuniziert. Bei einem derartigen aufwendiger gestalteten Mehrrechnersystem kann es zulässig sein, nicht nur den Ausfall einer einzigen Ein/Ausgabebaugruppe, sondern ggf. auch den Ausfall mehrerer Ein/
- 5 Ausgabebaugruppen zu tolerieren, wenn über die vorhandenen noch intakten Ein/Ausgabebaugruppen ein ordnungsgerechter Datenverkehr noch möglich ist. Die erfindungsgemäßen Verfahren sind insbesondere auch bei einem Zweivon-Drei/Rechnersystem vorteilhaft anwendbar.
- 10
- (Für die Datenübertragung zwischen den einzelnen Mehrrechnersystemen können beliebige Übertragungssysteme vorgesehen sein; vorzugsweise ist jedoch an die Verwendung linearer Bussysteme, insbesondere Ringbussysteme
- 15 gedacht.
- Dort, wo derartige Übertragungssysteme verdoppelt werden, geschieht dies überwiegend aus Verfügbarkeitsgründen. Bei dem erfindungsgemäßen Verfahren zum Betrieb
- 20 eines signaltechnisch sicheren Mehrrechnersystems dagegen wird die Verdoppelung der Bussysteme zunächst ausschließlich zur Erhöhung der Sicherheit beim Datenverkehr zwischen den Rechnersystemen verwendet, indem
- (die Daten mehrkanalig übertragen und die in den Ein/Ausgabebaugruppen jeweils anliegenden Daten vor ihrer An-
- 25 erkennung auf Übereinstimmung geprüft werden. Erst beim Ausfall eines Übertragungskanals zwischen zwei Mehrrechnersystemen wird die einem verdoppelten Übertragungssystem innenwohnende hohe Verfügbarkeit ausgenutzt und
- 30 die Datenübertragung vorübergehend einkanalig über das jeweils noch als ordnungsgerecht angesehene Übertragungssystem betrieben; dies ist nach der Lehre der Erfindung zulässig, sofern die dabei übermittelten Daten durch zusätzliche Maßnahmen gegen nicht erkennbare Feh-

0182134

-17-

VPA 84 P 2938 E

ler zusätzlich gesichert werden.

9 Patentansprüche

3 Figuren

Patentansprüche

1. Verfahren zum Betrieb eines signaltechnisch sicheren Mehrrechnersystems mit mindestens zwei signaltechnisch nicht sicheren Ein/Ausgabebaugruppen, über die die Rechner des Mehrrechnersystems mindestens zweikanalig Datentelegramme von und/oder zu anderen Rechnern und/oder sonstigen datenaufnehmenden, abgebenden oder verarbeitenden Systemen übertragen und über die sie von dort in Form von inhaltlich übereinstimmenden Telegrammen für die Ein/Ausgabebaugruppen durch Prüfdaten gesicherte Nutzdaten empfangen bzw. nach dort abgeben, d a - d u r c h g e k e n n z e i c h n e t , daß das sichere Mehrrechnersystem spätestens beim Erkennen von ihm von einer Datenquelle übermittelten ungleichen Daten in diesen Ein/Ausgabebaugruppen die dort abgelegten Daten einer Redundanzprüfung unterzieht und hieraus die Ein/Ausgabebaugruppe mit den fehlerhaften Daten bestimmt,
- daß das sichere Mehrrechnersystem dann die weitere Auswertung bzw. Fortschaltung von Daten über diese Ein/Ausgabebaugruppe im Verkehr mit dem System, von dem die fehlerbehafteten Daten stammen, unterbindet, daß das sichere Mehrrechnersystem die Datenquelle, von der es die ungleichen Daten erhalten hat, von dieser Maßnahme unterrichtet und diese Datenquelle dazu veranlaßt, die weitere Auswertung bzw. Fortschaltung von Daten über diejenige Ein/Ausgabebaugruppe, von der die als fehlerhaft erkannten Daten stammen, im Verkehr mit ihm zu unterbinden,
- daß das sichere Mehrrechnersystem diese Datenquelle im Verkehr mit ihm zur Abgabe von höherredundanten Daten auf eine der von ihr noch betriebenen, auf einen anderen Kanal geführten Ein/Ausgabebaugruppen veranlaßt und daß

sie das Einhalten der Redundanzbedingungen überwacht, daß das sichere Mehrrechnersystem auch selbst im Verkehr mit dem Datenempfänger der betreffenden Datenquelle die zu übertragenden Daten höherredundant erstellt, 5 über eine der von ihm noch betriebenen, auf einen anderen Kanal geführten Ein/Ausgabebaugruppen an den Datenempfänger übermittelt und den Datenempfänger zur Überwachung der Redundanzbedingungen veranlaßt, daß das sichere Mehrrechnersystem bei Nichteinhaltung 10 der Redundanzbedingungen durch die in einer der noch von ihm betriebenen Ein/Ausgabebaugruppen abgelegten Daten auch die weitere Auswertung bzw. Fortschaltung der dort abgelegten Daten unterbindet und daß das sichere Mehrrechnersystem die weitere Auswertung und Fortschaltung der in einer seiner noch be- 15 triebenen Ein/Ausgabebaugruppen abgelegten Daten unterbindet, wenn seit dem ersten Feststellen fehlerhafter Daten in einer seiner Ein/Ausgabebaugruppen eine definierte maximale Zeitdauer vergangen ist, ohne daß die 20 Störung in der bzw. den als defekt erkannten Ein/Ausgabebaugruppen bzw. dem betroffenen Übertragungskanal behoben wurde.

2. Verfahren zum Betrieb eines signaltechnisch sicheren 25 Mehrrechnersystems mit mindestens zwei signaltechnisch nicht sicheren Ein/Ausgabebaugruppen, über die die Rechner des Mehrrechnersystems mindestens zweikanalig Datentelegramme von und/oder zu anderen Rechnern und/oder sonstigen Daten aufnehmenden, abgebenden oder verarbei- 30 tenden Schaltmitteln übertragen und über die sie von dort in Form von inhaltlich übereinstimmenden Telegrammen für die Ein/Ausgabebaugruppen durch Prüfdaten gesicherte Nutzdaten empfangen bzw. nach dort abgeben,

- d a d u r c h g e k e n n z e i c h n e t ,
daß das sichere Mehrrechnersystem spätestens beim Erkennen von ungleichen Daten in diesen Ein/Ausgabebaugruppen die sort abgelegten Daten einer Redundanzprüfung unterzieht und hieraus die Ein/Ausgabebaugruppe mit den fehlerhaften Daten bestimmt,
daß das sichere Mehrrechnersystem dann die weitere Auswertung bzw. Fortschaltung von Daten über diese Ein/Ausgabebaugruppe unterbindet,
10 daß das sichere Mehrrechnersystem für die Dauer der Abschaltung einer seiner Ein/Ausgabebaugruppen die mit ihm kommunizierenden Datenquellen zur Abgaben von höherredundanten Daten auf eine der von ihm noch betriebenen auf einen anderen Kanal geführten Ein/Ausgabebaugruppen veranlaßt und das Einhalten der Redundanzbedingungen überwacht,
15 daß das sichere Mehrrechnersystem auch selbst im Verkehr mit Datenempfängern die zu übertragenden Daten höherredundant erstellt, über eine der von ihm noch betriebenen, auf einen anderen Kanal geführten Ein/Ausgabebaugruppen an die Datenempfänger übermittelt und die Datenempfänger zur Überwachung der Redundanzbedingungen veranlaßt,
20 daß das sichere Mehrrechnersystem bei Nichteinhaltung der Redundanzbedingungen durch die in einer der noch von ihm betriebenen Ein/Ausgabebaugruppen abgelegten Daten auch die weitere Auswertung bzw. Fortschaltung der dort abgelegten Daten unterbindet
und daß das sichere Mehrrechnersystem die weitere Auswertung und Fortschaltung der in einer seiner noch betriebenen Ein/Ausgabebaugruppen abgelegten Daten unterbindet, wenn seit dem ersten Feststellen fehlerhafter Daten in einer seiner Ein/Ausgabebaugruppen eine definierte maximale Zeitdauer vergangen ist, ohne daß die
30

Störung in der bzw. den als defekt erkannten Ein/Ausgabebaugruppen bzw. dem betroffenen Übertragungskanal behoben wurde.

- 5 3. Verfahren nach Anspruch 1 oder 2, d a d u r c h
g e k e n n z e i c h n e t , daß das sichere Mehrrech-
nersystem beim Feststellen von ungleichen Daten in sei-
nen mit inhaltlich gleichen Daten versorgten Ein/Ausgabe-
baugruppen und/oder beim Feststellen von Fehlern in den
10 höherredundant gesicherten Daten vor dem bleibenden
Sperrern der Auswertung der in den jeweils betroffenen
Ein/Ausgabebaugruppen abgelegten Daten mindestens eine
erneute Datenübermittlung anfordert.
- 15 4. Verfahren nach Anspruch 1, 2 oder 3, d a d u r c h
g e k e n n z e i c h n e t , daß das sichere Mehr-
rechnersystem beim Erkennen ungleicher Daten in den
durch die inhaltlich gleichen Telegramme belegten Ein/
Ausgabebaugruppen die weitere Auswertung bzw. die Fort-
20 schaltung von Daten aus den in den Vergleich jeweils
einbezogenen Ein/Ausgabebaugruppen unterbindet, wenn
die von ihm durchgeführten Redundanzprüfungen für die
Daten in diesen Ein/Ausgabebaugruppen zu dem Ergebnis
führen, daß die übermittelten Daten den Prüfbedingungen
25 genügen.
- 30 5. Verfahren nach Anspruch 2 oder 3, d a d u r c h
g e k e n n z e i c h n e t , daß das Mehrrechnersystem
beim Erkennen fehlerhafter Daten in einer seiner Ein/Aus-
gabebaugruppen mindestens die Datenquelle, von der die
fehlerhaft abgelegten Daten stammen, davon unterrich-
tet, von welcher ihrer Ein/Ausgabebaugruppen diese Da-
ten stammen und daß die betreffende Datenquelle darauf-
hin die weitere Ausgabe von Daten über diese Ein/Aus-

- gabebaugruppe unterbindet und die Ausgabe höherredun-
danter Daten über eine ihrer dann noch betriebenen
Ein/Ausgabebaugruppen auf einem anderen Kanal veran-
laßt bzw. auch ihrerseits das Einhalten der vorgege-
5 benen Redundanzbedingungen beim Datenempfang über die-
se Ein/Ausgabebaugruppe prüft.
6. Verfahren nach Anspruch 1, 2 oder 3, d a d u r c h
g e k e n n z e i c h n e t , daß die maximale Zeit-
10 dauer für die Betriebsfortführung des Mehrrechnersystems
ab dem ersten Feststellen fehlerhafter Daten in einer
seiner Ein/Ausgabebaugruppen abhängig gemacht ist von
der für die noch betriebenen Ein/Ausgabebaugruppen zu
erwartenden MTBF und der nach dem Auftreten der Störung
15 gewählten Datenredundanz.
7. Verfahren nach Anspruch 1, 2 oder 3, d a d u r c h ,
g e k e n n z e i c h n e t , daß die höherredundanten
Daten durch Verdoppelung der Datentelegramme und anti-
20 valente Darstellung der Daten in aufeinanderfolgenden
Telegrammen gebildet sind.
8. Einrichtung zur Durchführung des Verfahrens nach min-
destens einem der Ansprüche 1 bis 7, d a d u r c h
(
25 g e k e n n z e i c h n e t , daß für die Datenübertra-
gung ein mindestens zweikanaliges Bussystem (B1, B2)
vorgesehen ist und daß die zur Aufnahme jeweils inhalt-
lich gleicher Datentelegramme vorgesehenen Ein/Ausgabe-
baugruppen (z.B. E/A21, E/A22) des sicheren Mehrrech-
nersystems(RS2) an verschiedene Kanäle (B1 bzw. B2) des
30 Bussystems angeschlossen sind.

9. Einrichtung zur Durchführung des Verfahrens nach Anspruch 6, d a d u r c h g e k e n n z e i c h n e t, daß das sichere Mehrrechnersystem (R1, R2) ein signal-technisch sicheres Zeitglied (T1, T2) aufweist, das .
- 5 beim Sperren der Auswertung von in einer Ein/Ausgabe-
baugruppe abgelegten Daten einstellbar ist, nach Ablauf der ihm eingepprägten Schaltzeit die Auswertung der höherredundant gesicherten Daten unterbindet und das beim Feststellen von Übertragungs- oder Speicherfehlern
- 10 in diesen höherredundant gesicherten Daten die Auswertung dieser Daten unterbindet.

(1/2)

FIG 1

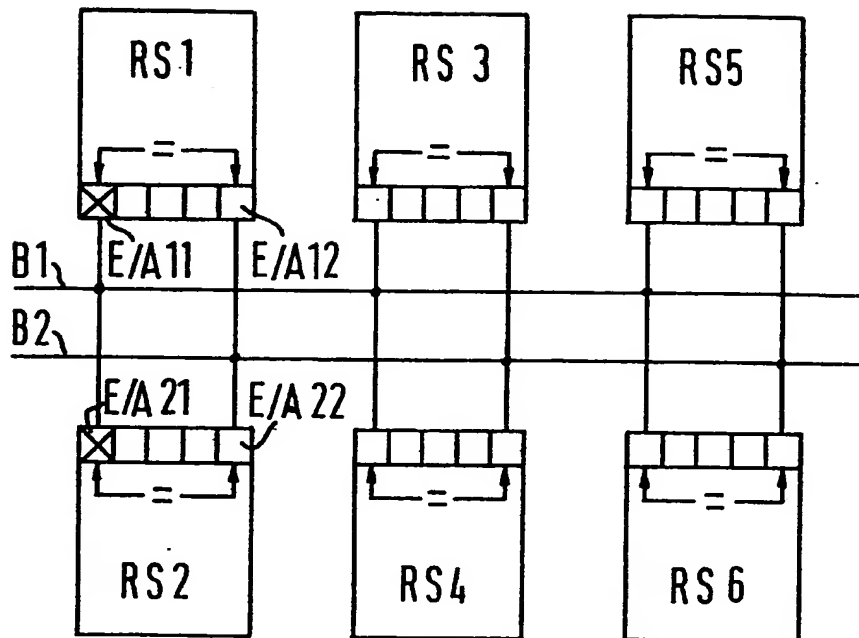
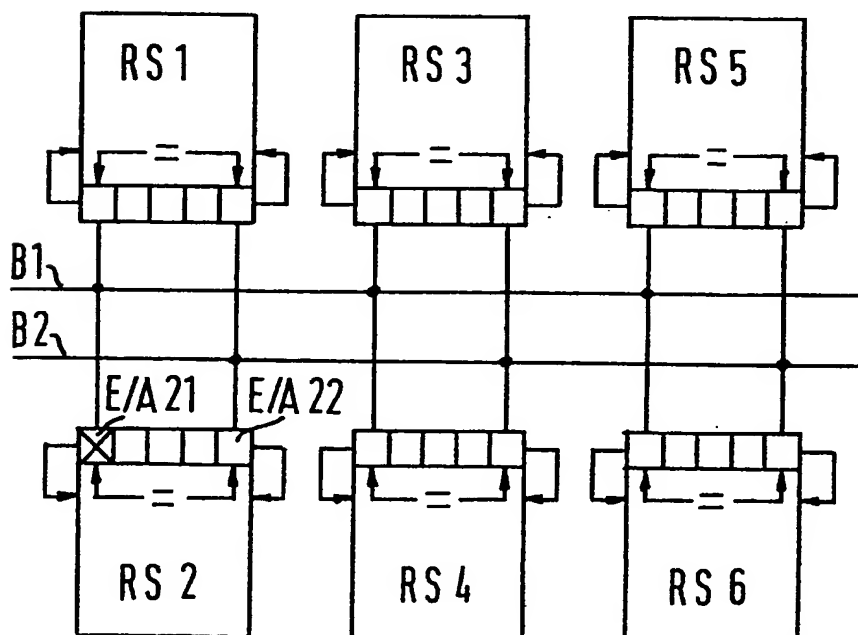
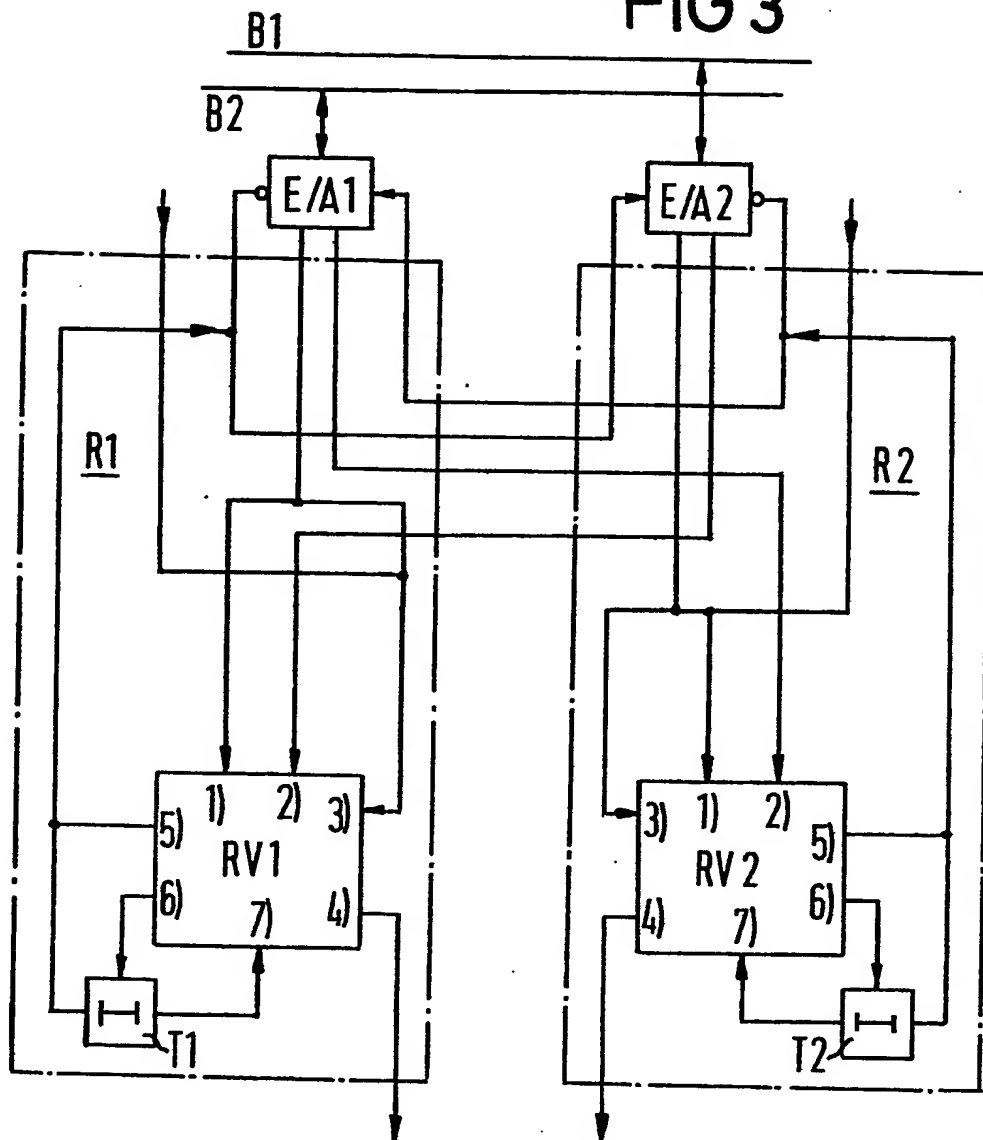


FIG 2



(2/2)

FIG 3



- 1) DATENVERGLEICH, REDUNDANZPRÜFUNG
- 2) DATENVERGLEICH, REDUNDANZPRÜFUNG
- 3) DATENEINGABE
- 4) DATENAUSGABE
- 5) SPERREN DER DATENAUSWERTUNG, ANFORDERN HÖHERREDUN-
DANTER DATEN, EINSTELLEN DES ZEITGLIEDES
- 6) RÜCKSTELLEN DES ZEITGLIEDES
- 7) ABBRUCH DES DATENVERKEHRS

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)